

U 9/890280

PCT/JP 00/00475

Best Available Copy

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

ETU

28.01.00  
REC'D 17 MAR 2000  
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて #3  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日  
Date of Application:

1999年 1月29日

出願番号  
Application Number:

平成11年特許願第021254号

出願人  
Applicant(s):

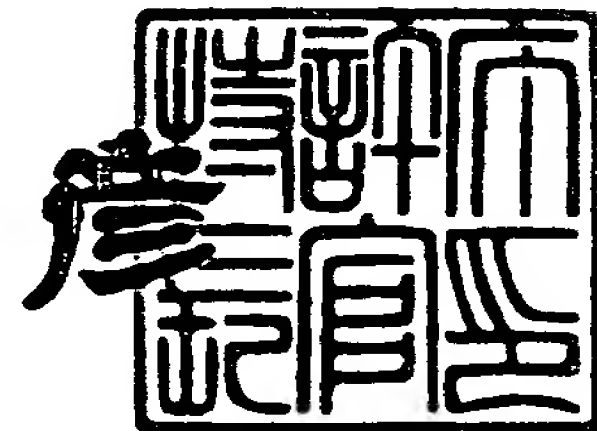
株式会社日立製作所

PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 3月 3日

特許庁長官  
Commissioner,  
Patent Office

近藤隆彦



出証番号 出証特2000-3011572

【書類名】 特許願

【整理番号】 K99000151

【提出日】 平成11年 1月29日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 公開鍵暗号方法

【請求項の数】 14

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

【氏名】 西岡 玄次

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100068504

【弁理士】

【氏名又は名称】 小川 勝男

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 公開鍵暗号方法

【特許請求の範囲】

【請求項 1】

送信者は、受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって、

(1) 鍵情報生成のステップとして、

【数 1】

- $p, q$ : prime numbers
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{p})$  . . . (数1)

なる前記秘密鍵  $(p, q, s)$  を作成し、さらに、

【数 2】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$  . . . (数2)
- $n = p^d q \quad (d \geq 1)$

なる前記公開鍵  $(n, g, h, k)$  を作成し (但し、 $k$  は  $p, q$  のビット長) ,

(2) 前記送信者は、前記公開鍵  $(n, g, h, k)$  を用いて、乱数  $r (0 < r < 2^{k-1})$  を選び、前記送信データ  $m (0 < m < 2^{k-1})$  について、

【数 3】

$$\begin{aligned} C &= mg^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (数3)$$

を計算し、 $C, D$  を前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵  $(p, q, s)$  を用いて、

【数 4】

$$m = CD^s \bmod p, \quad \dots (数4)$$

により、前記送信データ  $m$  を求めることを特徴とする公開鍵暗号方法。

## 【請求項 2】

送信者と受信者とが、暗号通信を行なうための鍵を共有する鍵共有方法であって、

(1) 鍵情報生成のステップとして、

## 【数 5】

- $p, q$ : prime numbers
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{p})$  . . . (数5)

なる秘密鍵  $(p, q, s)$  を作成し、さらに、

## 【数 6】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$
- $n = p^d q \quad (d \geq 1)$  . . . (数6)
- $f$ : one-way function

なる公開鍵  $(n, g, h, k, f)$  を作成し (但し、 $k$  は  $p, q$  のビット長)、

(2) 送信者は、前記公開鍵  $(n, g, h, k, f)$  を用いて、乱数  $r$  ( $0 < r < 2^{k-1}$ ) を選び、送信データ  $m$  ( $0 < m < 2^{k-1}$ ) について、

## 【数 7】

$$\begin{aligned} C &= mg^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots \text{(数7)}$$

を計算し、共有鍵  $K$  を  $K=f(m)$  により計算し、前記計算結果  $C, D$  を前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵  $(p, q, s)$  を用いて、

## 【数 8】

$$m = CD^s \bmod p, \quad \dots \text{(数8)}$$

により、前記送信データ  $m$  を求め、前記公開情報  $f$  を用いて前記共有鍵  $K$  を  $K=f(m)$  により計算する

ことを特徴とする鍵共有方法。

【請求項 3】

請求項 1 または請求項 2 における前記鍵情報の作成方法であって、

受信者は、有限群  $G = \{x \in \mathbb{Z}/(n) \mid x \text{ は可逆元} \}$  の大きな位数  $L$  を持つ元  $\xi$  を選ぶステップを備え（但し、 $\mathbb{Z}/(n)$  は  $n$  を法とする剰余環、 $L$  は  $\xi$  の位数の倍数でもよい）、整数  $\alpha$ 、 $\beta$  に対して、

【数 9】

$$g = \xi^\alpha \bmod n, \quad h = \xi^\beta \bmod n \quad \dots \text{(数 9)}$$

とするステップを備え、さらに、

【数 10】

$$\alpha + s\beta \equiv 0 \pmod{L} \quad \dots \text{(数 10)}$$

となるように前記秘密情報  $s$  を決めるステップを備えることを特徴とする鍵情報の作成方法。

【請求項 4】

送信者は、受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって、

(1) 受信者は、前記秘密鍵として、

【数 11】

- $p, q$ : prime numbers ... (数 11)
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{n})$

前記公開鍵として、

【数 12】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$
- $n = pq$  ... (数 12)

を作成するステップを備え、

(2) 送信者は、乱数  $r$  ( $0 < r < k$ ) を選び、送信データ  $m$  を、

【数 1 3】

$$\begin{aligned} C &= mg^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (\text{数} 1 3)$$

により、暗号化するステップを備え、

さらに、前記送信者は暗号文  $C$ ,  $D$  を受信者に送信するステップを備え、

(3) 受信者は、

【数 1 4】

$$m = CD^s \bmod n, \quad \dots (\text{数} 1 4)$$

により、前記送信データ  $m$  を復号化するステップを備える  
ことを特徴とする公開鍵暗号方法。

【請求項 5】

請求項 4 における鍵情報の作成方法であって、

受信者は、有限群  $G = \{x \in \mathbb{Z}/(n) \mid x \text{ は可逆元}\}$  の大きな位数  $L$  を持つ元  $\xi$  を選ぶ  
ステップを備え (但し、 $\mathbb{Z}/(n)$  は  $n$  を法とする剰余環、 $L$  は  $\xi$  の位数の倍数でもよい  
)、整数  $\alpha$ ,  $\beta$  に対して、

【数 1 5】

$$g = \xi^\alpha \bmod n, \quad h = \xi^\beta \bmod n \quad \dots (\text{数} 1 5)$$

とするステップを備え、さらに、

【数 1 6】

$$\alpha + s\beta \equiv 0 \pmod{L} \quad \dots (\text{数} 1 6)$$

となるように  $s$  を決めるステップを備える  
ことを特徴とする鍵情報の作成方法。

【請求項 6】

請求項 4 における前記受信者が該送信データ  $m$  を復号化するデータ復号化方法

であって、

受信者は、

【数 1 7】

$$\begin{aligned} m_1 &= CD^s \bmod p, & \dots (\text{数} 17) \\ m_2 &= CD^s \bmod q \end{aligned}$$

を計算するステップを備え、さらに、

【数 1 8】

$$\begin{aligned} a &\equiv 1 \pmod{p}, & a &\equiv 0 \pmod{q} \\ b &\equiv 0 \pmod{p}, & b &\equiv 1 \pmod{q} \end{aligned} \quad \dots (\text{数} 18)$$

なる整数  $a$ ,  $b$  に対して、

【数 1 9】

$$m = am_1 + bm_2 \bmod n \quad \dots (\text{数} 19)$$

にて、前記送信データ  $m$  を復号化するステップを備える  
ことを特徴とするデータ復号化方法。

【請求項 7】

送信者は、受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって、

(1) 鍵情報生成のステップとして、

【数 2 0】

- $p, q$ : prime numbers ... (数 20)
- $s_0, s_1 \in \mathbb{Z}$

なる前記秘密鍵  $(p, q, s_0, s_1)$  を作成し、さらに、

【数 2 1】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$  ... (数 21)
- $n = p^d q (d \geq 1)$

なる前記公開鍵  $(n, g, h, k)$  を作成し (但し,  $k$  は  $p, q$  のビット長であり,

【数 2 2】

$$s_i \alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1) \quad \dots (\text{数 2 2})$$

とする。),

(2) 前記送信者は, 前記公開鍵  $(n, g, h, k)$  を用いて, 乱数  $r$  ( $0 < r < 2^{k-1}$ ) を選び, 前記送信データ  $m$  ( $0 < m < 2^{k-1}$ ) について  $m = m_0 + m_1$  となるようにランダムに  $m_0, m_1$  を選ぶステップを備え, さらに,

【数 2 3】

$$\begin{aligned} C_0 &= m_0 g^{\alpha_0 r} \bmod n, \\ C_1 &= m_1 g^{\alpha_1 r} \bmod n, \\ D &= g^{\beta r} \bmod n, \end{aligned} \quad \dots (\text{数 2 3})$$

を計算し,  $(C_0, C_1, D)$  を前記受信者に送信し,

(3) 前記受信者は, 前記秘密鍵  $(p, q, s_0, s_1)$  を用いて,

【数 2 4】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \quad \dots (\text{数 2 4})$$

により, 前記送信データ  $m$  を求める

ことを特徴とする公開鍵暗号方法。

【請求項 8】

請求項 7 において,

前記送信者は, 前記送信データ  $m$  ( $0 < m < n$ ) に対して, 前記暗号化方法にて暗号文  $(C_0, C_1, D)$  を作成し, 当該暗号文  $(C_0, C_1, D)$  を受信者に送信し,

前記受信者は,

【数 2 5】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod n \quad \dots (\text{数 2 5})$$



にて復号化を行う

ことを特徴とする公開鍵暗号化方法。

【請求項 9】

送信者と受信者とが、暗号通信を行なうための鍵を共有する鍵共有方法であつて、

(1) 鍵情報生成のステップとして、

【数 2 6】

- $p, q$ : prime numbers
  - $s_0, s_1 \in \mathbb{Z}$
- ... (数 2 6)

なる秘密鍵  $(p, q, s_0, s_1)$  を作成し、さらに、

【数 2 7】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$
  - $n = p^d q (d \geq 1)$
  - $f$ : one-way function
- ... (数 2 7)

なる公開鍵  $(n, g, h, k, f)$  を作成し (但し、 $k$  は  $p, q$  のビット長であり、

【数 2 8】

$$s_i \alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1) \quad \dots \text{(数 2 8)}$$

とする。),

(2) 送信者は、前記公開鍵  $(n, g, h, k, f)$  を用いて、乱数  $r (0 < r < 2^{k-1})$  を選び、送信データ  $m (0 < m < 2^{k-1})$  について  $m = m_0 + m_1$  となるようにランダムに  $m_0, m_1$  を選ぶステップを備え、さらに、

【数 2 9】

$$\begin{aligned}
 C_0 &= m_0 g^{\alpha_0 r} \bmod n, \\
 C_1 &= m_1 g^{\alpha_1 r} \bmod n, \\
 D &= g^{\beta r} \bmod n,
 \end{aligned}
 \quad \dots (数 2 9)$$

を計算し、共有鍵 $K$ を $K=f(m)$ により計算し、前記計算結果 $(C_0, C_1, D)$ を前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵 $(p, q, s_0, s_1)$ を用いて、

【数 3 0】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \quad \dots (数 3 0)$$

により、前記送信データ $m$ を求め、前記公開情報 $f$ を用いて前記共有鍵 $K$ を $K=f(m)$ により計算する

ことを特徴とする鍵共有方法。

【請求項 1 0】

送信者は、受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって、

(1) 鍵情報生成のステップとして、

【数 3 1】

- $s \in \mathbb{Z}, \quad gh^s = 1 \ (\in H) \quad \dots (数 3 1)$
- $H$ : subgroup of  $G$

なる前記秘密鍵 $(s, H)$ を作成し、さらに、

【数 3 2】

- $g, h \in G \quad \dots (数 3 2)$
- $G$ : finite group

なる前記公開鍵 $(g, h, G)$ を作成し、

(2) 前記送信者は、前記公開鍵  $(g, h, G)$  を用いて、乱数  $r$  を選び、前記送信データ  $m$  ( $m \in H$ ) について、暗号文  $C, D$  を

【数 3 3】

$$\begin{aligned} C &= m^t g^r (\in G), \\ D &= h^r (\in G) \end{aligned} \quad \dots (\text{数 } 33)$$

にて計算し、該暗号文  $C, D$  を前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵  $(s, H)$  を用いて、

【数 3 4】

$$m^t = CD^s (\in H), \quad \dots (\text{数 } 34)$$

を計算し、これより前記送信データ  $m$  を求める

ことを特徴とする公開鍵暗号方法。

【請求項 1 1】

送信者と受信者とが、暗号通信を行なうための鍵を共有する鍵共有方法であって、

(1) 鍵情報生成のステップとして、

【数 3 5】

- $s \in \mathbb{Z}, gh^s = 1 (\in H)$
  - $H$  : subgroup of  $G$
- ... (数 35)

なる秘密鍵  $(s, H)$  を作成し、さらに、

【数 3 6】

- $g, h \in G$
  - $G$  : finite group
  - $f$  : one-way function
- ... (数 36)

なる公開鍵  $(g, h, G)$  を作成し、

(2) 送信者は、前記公開鍵  $(g, h, G)$  を用いて、乱数  $r$  を選び、前記送信データ

$m$  ( $m \in H$ ) について、暗号文  $C, D$  を

【数 3 7】

$$\begin{aligned} C &= m^t g^r \ (\in G), \\ D &= h^r \ (\in G) \end{aligned} \quad \dots (\text{数 } 37)$$

にて計算し、共有鍵  $K$  を  $K=f(m)$  により計算し、該暗号文  $C, D$  を前記受信者に送信し

(3) 前記受信者は、前記秘密鍵  $(s, H)$  を用いて、

【数 3 8】

$$m^t = CD^s \ (\in H), \quad \dots (\text{数 } 38)$$

を計算し、前記送信データ  $m$  を求め、公開情報  $f$  を用いて共有鍵  $K$  を  $K=f(m)$  により計算する

ことを特徴とする鍵共有方法。

【請求項 1 2】

送信者は、受信者の公開鍵を用いて送信データを暗号化し、受信者は、前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって、

(1) 鍵情報生成のステップとして、

【数 3 9】

- $p, q$ : prime numbers ... (数 39)
- $s \in \mathbb{Z} \ (gh^s \equiv 1 \pmod{pq})$

なる前記秘密鍵  $(p, q, s)$  を作成し、さらに、

【数 4 0】

- $g, h, k \in \mathbb{Z} \ (0 < g, h < n)$  ... (数 40)
- $n = p^d q \ (d \geq 1)$

なる前記公開鍵  $(n, g, h, k)$  を作成し (但し、 $k$  は  $p, q$  のビット長) ,

(2) 前記送信者は、前記公開鍵  $(n, g, h, k)$  を用いて、乱数  $r$  ( $0 < r < 2^{k-1}$ ) を選び、前記送信データ  $m$  ( $0 < m < 2^{k-1}$ ) について、暗号文  $C, D$  を

【数 4 1】

$$\begin{aligned} C &= m^2 g^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (数4 1)$$

にて計算し、該暗号文  $C, D$  を前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵  $(p, q, s)$  を用いて、

【数 4 2】

$$m^2 = CD^s \bmod pq, \quad \dots (数4 2)$$

を計算し、前記送信データ  $m$  を求める

ことを特徴とする公開鍵暗号方法。

【請求項 1 3】

送信者と受信者とが、暗号通信を行なうための鍵を共有する鍵共有方法であつて、

(1) 鍵情報生成のステップとして、

【数 4 3】

- $p, q$ : prime numbers ... (数4 3)
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{pq})$

なる秘密鍵  $(p, q, s)$  を作成し、さらに、

【数 4 4】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$
- $n = p^d q (d \geq 1)$  ... (数4 4)
- $f$ : one-way function

なる公開鍵  $(n, g, h, k, f)$  を作成し (但し、 $k$  は  $p, q$  のビット長)、

(2) 送信者は、前記公開鍵  $(n, g, h, k)$  を用いて、乱数  $r$  ( $0 < r < 2^{k-1}$ ) を選び、送信データ  $m$  ( $0 < m < 2^{k-1}$ ) について、暗号文  $C, D$  を、

【数 4 5】

$$\begin{aligned} C &= m^2 g^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (数45)$$

にて計算し、共有鍵Kを $K=f(m)$ により計算し、前記計算結果C,Dを前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵 $(p,q,s)$ を用いて、

【数 4 6】

$$m^2 = CD^s \bmod pq, \quad \dots (数46)$$

を計算し、前記送信データmを求め、前記公開情報fを用いて前記共有鍵Kを $K=f(m)$ により計算する

ことを特徴とする鍵共有方法。

【請求項 1 4】

請求項12において、

前記送信者は、前記送信データm ( $0 < m < n$ ) に対して、前記暗号化方法にて前記暗号文C,Dを作成し、前記暗号文C,Dを受信者に送信し、

前記受信者は、

【数 4 7】

$$m^2 = CD^s \bmod n, \quad \dots (数47)$$

を計算し、前記送信データmの復号化を行う

ことを特徴とする公開鍵暗号化方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、公開鍵暗号を用いた暗号通信方法および装置に関する。

【0 0 0 2】

【従来技術】

現在まで、様々な公開鍵暗号方式が提案されている。なかでも、

文献1 「R. L. Rivest, A. Shamir, L. Adleman. :A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1987.」

に記載されている方法が最も有名であり, 最も実用化されている公開鍵暗号である。その他には,

文献2 「T.ElGamal.:A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp.469-472(1985)」

に記載されている暗号方法,

文献3 「M.O.Rabin.: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」に記載されている暗号方法,

文献4 「V. S. Miller. :Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS 218, Springer - Verlag, pp.417-426 (1985)」,

文献5 「N. Koblitz.: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987)」

等に記載の楕円曲線を用いた暗号方法,

文献6 「S. Goldwasser and S.Micali.: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984)」に記載されている暗号方法,

文献7 「M.Blum and S.Goldwasser.: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS 196, Springer - Verlag, pp.289-299 (1985)」に記載されている暗号方法,

文献8 「S.Goldwasser and M.Bellare.: Lecture Notes on Cryptography, <http://www-cse.ucsd.edu/users/mihir/> (1997)」に記載されている暗号方法,

文献9 「R. Cramer and V. Shoup.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS, Springer - Verlag, pp.13-25 (1998)」に記載されている暗号方法,

などが知られている。最近では,

文献10「T. Okamoto and S. Uchiyama, A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS, Springer Verlag, pp.308-318 (1998)」

の中で素因数分解問題の困難性と等価な（完全解読に対する）安全性を主張する公開鍵暗号方式が提案されている。

【0003】

【発明が解決しようとする課題】

文献1に開示されている暗号方法の安全性は、素因数分解問題の困難性を仮定しているが、等価性は示されていない。すなわち、素因数分解問題を解ければ文献1の暗号方法を破ることができるが、逆は証明されていない。素因数分解問題よりも簡単な問題を解くことで文献1の暗号方法を破ることが出来る可能性は残されている。

【0004】

さらに文献1の暗号方法は、確定的な暗号であるため、鍵が同一である場合、同一の平文に対する暗号文は常に同一になる。そのままで使用すると、複数の暗号文から平文の同一性を判断することが可能になるので、これを防ぐためには運用時は乱数情報を付加するという別処理が必要になり、効率が悪い。

【0005】

これに対して、文献10に開示されている暗号方法では、受動的攻撃に対して暗号文から平文を求めること（完全解読）は素因数分解問題の困難性と等価であることが証明されており、これにより安全性を保証している。さらに、同一の平文であっても暗号文が変化する確率暗号であるため、文献1の暗号方法のような問題や、別処理の必要性はない。

【0006】

また、文献10の暗号方法における部分解読に対する安全性（semantic security）は、文献10中にて定義されているp-部分群問題の困難性と等価であるとして、その安全性が主張されている。しかしながら、この問題は未だ十分な議論がなされておらず、その困難性については知られていない。つまり、p-部分群問題を解く効率的なアルゴリズムが見つければ、文献10の暗号方法の部分解読を効率的



に行うことが出来てしまい、その安全性は保証できなくなる。

【 0 0 0 7 】

一般に、暗号の安全性を保証するためには、素因数分解問題や離散対数問題など計算量的困難性について十分議論されている問題との等価性を示すことが望ましい。

【 0 0 0 8 】

また、文献 9 に記載の暗号方法は、文献 2 に記載の暗号方法を用いて作成した暗号文に、暗号前のメッセージを知らないと作成できない「メッセージ情報」を付与するものである。このメッセージ情報が暗号文に対応する場合だけ正当な暗号文として対処し、そうでない場合は拒否するという仕組みであり、このメッセージ情報処理の処理量が多い。。

【 0 0 0 9 】

一方、携帯型情報処理機器の普及やネットワーク環境の発展などにより、これら携帯型情報処理機器を用いて電子商取引を行うことが増えてくると予想されている。これら情報機器においては、計算能力が限られている反面、電子商取引では、複雑なプロトコルのために、元々データ量が多い。したがって、暗号化に伴うデータ量を減らすよりは、計算負荷を減らす方が望まれる場合がある。

【 0 0 1 0 】

本発明の目的は、計算量的にその解決の困難性が予測されている数学的問題と等価な（または以上の）安全性を持つ、すなわち、安全性が保証された、公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、それぞれの方法を実行するプログラム、装置またはシステムを提供することである。

【 0 0 1 1 】

また、本発明のより具体的な目的は、受動的攻撃による解読の困難性が、計算量的困難性が予想されている数論的問題(NP問題)と等価（または以上）であり、安全性が保証された公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、これらの方法を実行するプログラム、装置またはシステムを提供することである。

## 【0 0 1 2】

本発明の他の目的は、上記、安全性が保証された暗号方法を用いて、能動的な攻撃方法である選択暗号文攻撃を許さない環境を提供し、あらゆる攻撃に対して安全性を確保することである。

## 【0 0 1 3】

本発明の他の目的は、上記、安全性が保証された暗号方法において、確率的暗号方法を提供することである。

## 【0 0 1 4】

また、本発明の他の目的は、計算負荷が小さく、携帯型情報処理機器など計算能力が限られた装置であっても高速処理が可能な、公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、それぞれの方法を実行するプログラム、装置またはシステムを提供することである。

## 【0 0 1 5】

## 【課題を解決するための手段】

上記目的を達成するため、本発明は、以下の特徴を備える。

## 【0 0 1 6】

(1) 受動的攻撃、より具体的には、公開鍵暗号における既知平文攻撃、選択平文攻撃や暗号文攻撃、のもとでの、暗号文から平文を求める完全解読は、素因数分解問題を解くよりも困難である。これにより、本発明が提供する暗号方法への、全文解読を目的とする受動的攻撃に対する安全性を、素因数分解問題の困難性を根拠とする従来の暗号方法よりもさらに強く保証する。

## 【0 0 1 7】

(2) 受動的攻撃の元での部分解読の困難性は、Diffie-Hellman決定問題の困難性と等価である (Diffie-Hellman決定問題の困難性については、文献11「V.Shoup.: Lower bounds for discrete logarithms and related problems. In Advances in Cryptology-Eurocrypt'97 (1997)」において、その困難性が予想されている)。

## 【0 0 1 8】

これによって、本発明が提供する暗号化方法への部分解読を目的とする受動的

攻撃に対する安全性が保証される。さらに部分解読攻撃に対する安全性を保証されれば、完全解読攻撃に対する安全性もまた保証される。

【0 0 1 9】

(3) 暗号化の過程において、確率的な情報を用いた処理を施す。これにより、暗号化する平文に対して確率的情報を挿入する必要がない。すなわち、本発明が提供する暗号化方法は、同一の平文であっても、暗号文の値が変化する確率暗号である。

【0 0 2 0】

(4) 暗号化処理を行う者（以下、暗号化者という）および復号化処理を行う者（以下、復号化者という）の計算負荷が小さく、高速な処理が可能である。

【0 0 2 1】

(5) 本発明が提供する暗号化方法に、実用的な一方向性関数を組み合わせ、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作ることによって、その安全性を確保する。

【0 0 2 2】

具体的には、本発明が提供する方法は、以下のステップから成るものであり、また、本発明が提供する装置は、以下のステップを実行する手段またはプログラムを備えるものである。

【0 0 2 3】

[鍵情報生成]

秘密鍵として、

【0 0 2 4】

【数 4 8】

- $p, q$ : prime numbers ... (数 4 8)
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{n})$

【0 0 2 5】

公開鍵として、

【 0 0 2 6 】

【数 4 9】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$  . . . (数49)
- $n = p^d q (d \geq 1)$

【 0 0 2 7 】

を作成する（但し、 $L$ は $g$ の位数、 $k$ は $p, q$ のビット長を表す）。

【 0 0 2 8 】

[暗号化]

送信者は、乱数 $r$  ( $0 < r < 2^{k-1}$ ) を選び、送信データ $m$  ( $0 < m < 2^{k-1}$ ) を、

【 0 0 2 9 】

【数 5 0】

$$\begin{aligned} C &= m^2 g^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots \text{(数50)}$$

【 0 0 3 0 】

により、暗号化する。さらに、送信者は暗号文 $C, D$ を受信者に送信する。

【 0 0 3 1 】

[復号化]

受信者は、

【 0 0 3 2 】

【数 5 1】

$$m^2 = CD^s \bmod pq, \quad \dots \text{(数51)}$$

【 0 0 3 3 】

により、送信データ $m$ を復号化する。

【 0 0 3 4 】

【発明の実施の形態】

以下、図面を用いて、本発明の実施例について説明する。

【 0 0 3 5 】

なお、本明細書においては、上記暗号化者を送信者、復号化者を受信者、暗号化の対象となる平文データ  $m$  を送信データ  $m$  ともいう。

【 0 0 3 6 】

図 1 は、本発明の各実施例を実現するシステム構成を示す図である。

【 0 0 3 7 】

図 1 において、ネットワーク 300 に暗号化者が使用するコンピュータ（以下、暗号化者側装置、または送信者側装置ともいう）100、および、復号化者が使用するコンピュータ（以下、復号化者側装置、または受信者側装置ともいう）200、および、第 3 者が使用するコンピュータ（以下、第 3 者側装置ともいう）400 が接続されている。

【 0 0 3 8 】

暗号化者側装置 100 は、CPU 101、メモリ 102、通信装置 103、バス 104 によって構成され、さらにディスプレイ 106、および、キーボード 107 がバス 104 に接続されている。

【 0 0 3 9 】

暗号化者側装置 100 のメモリ 102 は、メモリ 102 は半導体記憶装置やハードディスクなどの二次記憶装置で構成されるものであり、以下の各実施例に示す、各種情報と、CPU 101 が実行するプログラム（手段という）と、キーボード 107 や可搬型記憶媒体または通信回線 300 を介して入力される、暗号化の対象となる平文データ（送信データ）と、送信される暗号文が保存される。

【 0 0 4 0 】

同様に、復号化者側装置 200 には、CPU 201、メモリ 202、通信装置 203、バス 204 によって構成され、さらにディスプレイ 206、キーボード 207、および、復号化者の所有する、IC カードと通信をすることができる IC カードリーダー・ライター 205 がバス 204 に接続されている。

## 【 0 0 4 1 】

復号化者側装置200のメモリ202は、半導体記憶装置やハードディスクなどの二次記憶装置で構成されるものであり、以下の各実施例に示す、各種情報と、CPU201が実行するプログラム（手段という）と、復号化の対象となる暗号文と、復号化され、ディスプレイ206や通信回線300に出力される平文データ（送信データ）が保存される。

## 【 0 0 4 2 】

## （実施例 1）

本実施例は、メッセージの送信者 A が受信者 B に対して、送信データ  $m$  ( $0 < m < 2^{k-1}$ ) を暗号通信によって送信する場合について説明する。

## 【 0 0 4 3 】

## 1. 鍵情報生成処理

予め、受信者側装置200内の鍵生成手段2001は、

## 【 0 0 4 4 】

## 【数 5 2】

- $p, q$ : prime numbers ... (数5 2)
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{p})$

## 【 0 0 4 5 】

なる秘密情報  $(p, q, s)$  を作成し、

## 【 0 0 4 6 】

## 【数 5 3】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$  ... (数5 3)
- $n = p^d q \quad (d \geq 1)$

## 【 0 0 4 7 】

なる公開情報  $(n, g, h, k)$  （但し、 $k$  は  $p, q$  のビット長を表す。）を作成する。

。

【0048】

そして上記公開情報2006を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。上記秘密情報2007は、メモリ202に格納する。

【0049】

## 2. 暗復号化处理

(1) 送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて、整数 $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選ぶ。さらに、第3者装置400あるいは、受信者側装置200から得られる上記公開情報2006と、べき乗算手段1002, 剰余演算手段1003とを用いて、送信データ $m$  ( $0 < m < 2^{k-1}$ ) に対する暗号文 $C$ ,  $D$ を

【0050】

【数54】

$$\begin{aligned} C &= mg^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (数54)$$

【0051】

にて計算する。

【0052】

さらに、暗号文 $C$ ,  $D$ を、通信装置103を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0053】

(2) 受信者側装置200において、復号化手段2004は、べき乗算手段2002, 剰余演算手段2003と、保持されている上記秘密情報2007とを用いて、

【0054】

【数55】

$$m = CD^s \bmod p, \quad \dots (数55)$$

【 0 0 5 5 】

にて、暗号文 C, D から送信データ m を復号化する。

【 0 0 5 6 】

上記文献 9 では、文献 2 に記載の暗号方法において、semantic security が Diffie - Hellman 決定問題の困難性のもとで示すことができると、指摘されている。これと同様にして、本実施例の方法を用いれば、受動的な暗号文攻撃に対して、平文の部分情報(少なくとも任意の 1 ビット)を求める部分解読が Diffie - Hellman 決定問題と同等に困難であること、すなわち、本発明の方法は、Semantically secure であることを証明することが出来る。

【 0 0 5 7 】

なお、Diffie-Hellman 決定問題とは、

【 0 0 5 8 】

【数 5 6】

$$R : (g^x \bmod n, g^y \bmod n, g^z \bmod n) \quad g, x, y, z \text{ are random} \quad \dots (\text{数} 5 6)$$

【 0 0 5 9 】

からのシーケンスと

【 0 0 6 0 】

【数 5 7】

$$D : (g^x \bmod n, g^y \bmod n, g^{xy} \bmod n) \quad g, x, y, z \text{ are random} \quad \dots (\text{数} 5 7)$$

【 0 0 6 1 】

からのシーケンスのいずれか一方がランダムに与えられたとき、どちらからのシーケンスかを言い当てる問題である。

【 0 0 6 2 】

本実施例による方法では、適当な秘密の整数  $\alpha$  に対して、



【 0 0 6 3 】

【数 5 8】

$$h \equiv g^{\alpha} \pmod{n} \quad \dots (数58)$$

【 0 0 6 4 】

と書けるとき、 $g, \alpha, m_0, m_1$ をランダムに選ぶと、

【 0 0 6 5 】

【数 5 9】

$$(C/m_i \bmod n, h, D) \quad (0 \leq i \leq 1) \quad \dots (数59)$$

【 0 0 6 6 】

なるシーケンスはそれぞれRおよびDの分布を示す（但し、暗号文C,Dは $m_0$ か $m_1$ のどちらかの暗号文）。このとき、本実施例の方法に対して部分解読を行う問題は、このDiffie-Hellman決定問題を解くことと同値であることが示される。

【 0 0 6 7 】

これにより、部分解読の困難性とDiffie-Hellman決定問題の困難性が等価であることにより、その安全性を保証することができる。さらに、部分解読に対する安全性を保証することができるため、完全解読に対する安全性も、同じく保証することができる。

【 0 0 6 8 】

以上述べたように、本発明の方法は、受動的攻撃に対する安全性を保証することができる。

【 0 0 6 9 】

また、後述するように、本発明による暗号化、復号化方法は、モジュラー積の個数という観点からみて非常に効率がよいことがわかる。

さらに、送信者側において、暗号化处理の際、乱数 $r$ が導入されているため、本発明の方法は、確定的ではなく、確率的である。よって、新たに乱数情報を含ませることなく、暗号文から平文の同一性を判断することは困難であり、文献1の方法などと比較して安全性を向上させている。言い換えると、安全性を向上さ

せるために乱数情報を新たに含ませる必要がなく、運用時の処理を簡単にすることができる。

#### 【0 0 7 0】

なお、上記公開情報は、必ずしも受信者が作成する必要はなく、システム構成によっては、管理者である第3者が作成して、システム参加者へ配布してもよいものである。

#### 【0 0 7 1】

##### (実施例 2)

本実施例は、上記実施例 1 で述べた方法に、さらに、実用的な一方向性関数を組み合わせるものである。これにより、送信者と受信者の間で鍵共有を行うこと(すなわち、共通鍵暗号方法に用いる鍵を配送すること)を可能にする。また、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作り、能動的攻撃に対する安全性を確保する。

#### 【0 0 7 2】

本実施例では、図 1 のシステム構成において、図 2 に示す IC カード 500 を、受信者側装置 200 の IC カードリーダライタ 205 に挿入して用いる。このとき、受信者側装置 200 の復号化手段 2004、べき乗算手段 2002、剰余演算手段 2003 はなくてもよい。

また、一方向性関数手段 2008 を新たに送信者側装置 100 内に設ける。

また、配送された(または共有する)鍵を用いて、同時に、あるいは別途送受するデータを、おのこの暗号化、復号化する機能を有するアプリケーション A プログラム 1005、アプリケーション B プログラム 2005 を、図 1 に示すように備えるものとする。

#### 【0 0 7 3】

##### 1. 鍵情報生成処理

予め、受信者側装置 200 内の鍵生成手段 2001 は、

【 0 0 7 4 】

【数 6 0】

- $p, q$ : prime numbers
- $s \in \mathbf{Z} (gh^s \equiv 1 \pmod{p})$  . . . (数 6 0)

【 0 0 7 5 】

なる秘密情報  $(p, q, s)$  を作成し,

【 0 0 7 6 】

【数 6 1】

- $g, h, k \in \mathbf{Z} (0 < g, h < n)$
- $n = p^d q \quad (d \geq 1)$  . . . (数 6 1)
- $f$  : one-way function

【 0 0 7 7 】

なる公開情報  $(n, g, h, k)$  (但し,  $k$  は  $p, q$  のビット長を表す。) を作成する。

【 0 0 7 8 】

そして、公開情報として  $n, g, h, k$  を通信回線 300 などを通して出力し、受信者側装置 200 へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関 (たとえば第 3 者側装置 400) への登録など、周知の方法を用いることが可能である。その他の情報は、メモリ 202 に格納する。

【 0 0 7 9 】

## 2. 暗復号化处理

(1) 送信者側装置 100 内の暗号化手段 1004 は、乱数生成手段 1001 を用いて整数  $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選び、公開情報 2006、べき乗算手段 1002、剰余演算手段 1003 を用いて、送信データ  $m$  ( $0 < m < 2^{k-1}$ ) に対する暗号文  $C, D$  を

【 0 0 8 0 】

【数 6 2】

$$\begin{aligned} C &= mg^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (数 6 2)$$

【 0 0 8 1 】

にて計算する。

【 0 0 8 2 】

さらに、暗号文 C、D を通信装置 103 を用いて通信回線 300 を介して受信者 B の受信者側装置 200 に送信する。

【 0 0 8 3 】

さらに、送信者側装置 100 内の一方向性関数手段 2008 は、公開情報である一方向性関数  $f$  から共通鍵  $K$  を  $K=f(m)$  により計算する。必要に応じて、アプリケーション A プログラム 1005 は、共通鍵  $K$  を用いて暗号化計算を行う。

【 0 0 8 4 】

(2) 受信者側装置 200 では、IC カード 500 内の復号化手段 5004 が、メモリ 502 に保持されている上記秘密情報 2007 と、べき乗算手段 5002、剰余演算手段 5003 とを用いて、

【 0 0 8 5 】

【数 6 3】

$$m = CD^s \bmod p, \quad \dots (数 6 3)$$

【 0 0 8 6 】

にて、暗号文 C、D から送信データ  $m$  を復号化する。

【 0 0 8 7 】

さらに、IC カード 500 内の一方向性関数手段 5008 は、公開情報である一方向性関数  $f$  から共通鍵  $K$  を  $K=f(m)$  により計算し、IC カード 500 から  $m$  を出力することなく、 $K$  を受信者側装置 200 に出力する。

【 0 0 8 8 】

受信者側装置200内のアプリケーションBプログラム2005は、この共通鍵Kを用いて、同時に、あるいは、別途送付される、共通鍵Kで暗号化されたデータを復号化する。

【 0 0 8 9 】

上述のように、本実施例は、実用的な一方向性関数を組み合わせて使用することにより、平文データ $m$  ( $0 < m < 2^{k-1}$ ) を外部へ出力しない。

【 0 0 9 0 】

このように、ICカード(または、計算機カード)など個人が携帯する周辺機器内部で、暗号化、復号化処理を行うことで、選択暗号文攻撃を許さない、すなわち能動的攻撃に対しても安全な環境を作ることができる。

【 0 0 9 1 】

また、メッセージそのものを、本発明による公開鍵暗号方法を用いて送信する構成においては、本実施例のアプリケーションBプログラム2005が、復号化したメッセージ(平文データ $m$ )を所定の知識/ルールによって解釈して、意味のないメッセージが復号化されたと判断した場合、そのメッセージを秘密のうちに消去するなどして、他に知れないようにすることで、能動的攻撃を許さない環境を作ることができる。

【 0 0 9 2 】

上述のように、本実施例は、実用的な一方向性関数を組み合わせて使用することにより、さらに、能動的攻撃に対しても安全な環境を作るものである。

【 0 0 9 3 】

(実施例 3)

本実施例は、実施例1および実施例2において、送信者の計算効率を高めるための鍵情報生成の方法について述べる。

【 0 0 9 4 】

受信者側装置200内の鍵生成手段2001は、有限群 $G = \{x \in \mathbb{Z}/(n) \mid x \text{ は可逆元} \}$ の大きな位数 $L$ を持つ元 $\xi$ を選び(但し、 $\mathbb{Z}/(n)$ は $n$ を法とする剰余環、 $L$ は $\xi$ の位数の倍数でもよい)、整数 $\alpha$ 、 $\beta$ に対して、

【 0 0 9 5 】

【数 6 4】

$$g = \xi^{\alpha} \bmod n, \quad h = \xi^{\beta} \bmod n \quad \dots (\text{数} 64)$$

【 0 0 9 6 】

とする。さらに、

【 0 0 9 7 】

【数 6 5】

$$\alpha + s\beta \equiv 0 \pmod{L} \quad \dots (\text{数} 65)$$

【 0 0 9 8 】

となるように  $s$  を決める。

【 0 0 9 9 】

このとき、 $g$ 、 $h$ において、小さな整数  $k$  ( $k \geq 2$ ) に対して

【 0 1 0 0 】

【数 6 6】

$$h = g^k \bmod n \quad \dots (\text{数} 66)$$

【 0 1 0 1 】

とすると、送信者側の計算効率をさらに高めることができる。

【 0 1 0 2 】

ここで、小さな整数  $k$  を選ぶことは、 $k$  を公開情報にすることに等しくなり、部分解読に対する安全性と Diffie-Hellman 決定問題の困難性との等価性への保証がなくなることがある。しかし、これは、部分解読に対して弱いということを意味するものではない。

【 0 1 0 3 】

また、公開鍵  $g, h$  が小さな値となるように  $p, q, \xi, \alpha, \beta$  を選ぶことにより、公開鍵のサイズを小さくすることが可能である。より具体的には、 $g$  を大きな奇数（例えば素数） $L$  を位数とする小さな値を選び、

【 0 1 0 4 】

【数 6 7】

$$h = g^2 \bmod n$$

... (数 6 7)

【 0 1 0 5 】

とする。さらに、

【 0 1 0 6 】

【数 6 8】

$$2s + 1 \equiv 0 \pmod{L}$$

... (数 6 8)

【 0 1 0 7 】

にて  $s$  を計算する。

【 0 1 0 8 】

送信者側装置 100 内の暗号化手段 1004 は、べき乗算手段 1002、剰余演算手段 1003 を用いて、

【 0 1 0 9 】

【数 6 9】

$$W = g^r \bmod n$$

... (数 6 9)

【 0 1 1 0 】

を計算し、さらに、

【 0 1 1 1 】

【数 7 0】

$$C = mW \bmod n,$$

$$D = W^2 \bmod n$$

... (数 7 0)

【 0 1 1 2 】

により暗号文を計算することで、送信者側装置の計算負担を少なくすることが出来る (図 4)。

## 【0 1 1 3】

また、 $d$  ( $d \geq 1$ ) の値を  $n$  の素因数分解が困難である範囲において、大きく選ぶことで、 $n$  のビット数が一定の場合、 $p$  のビット数が小さくなるため、復号化処理を高速に行うことが出来る。この  $d$  の値を、第3者側装置400あるいは、受信者側装置200にて管理すれば、計算機能力の発展、素因数分解に必要とされる計算時間と安全性との関係などによって、変えることが可能である。

## 【0 1 1 4】

図5に、代表的な実用的公開鍵暗号方法（それぞれの方法については、従来の技術の項にて述べた上記各文献に記載されている）とのモジュラー積の個数による効率性の比較を示す。ここにあるデータの従来方式に関するものは文献10から引用したものであり、また、本発明による方式では、文献10にて提案されている暗号方法と同様の底となるように  $d=2$  としている。

## 【0 1 1 5】

なお、図5に示す本発明による効率性は、送信側より受信側の方が、負荷が少ないが、送信側では後述するように、送信データを用いない計算部分を、前処理とすることが可能である。この結果、送信側の効率も大幅に向上させることができる。

## 【0 1 1 6】

## (実施例 4)

本実施例は実施例1の変形例である。

本実施例では、実施例1に対して、 $n$  を法とした剰余環の上で復号化を行うことにより、送信データ  $m$  を長くすることを可能とし、また、選択暗号文攻撃に対する対策を行っている。

## 【0 1 1 7】

## 1. 鍵情報生成処理

予め、受信者側装置200内の鍵生成手段2001は、



【 0 1 1 8 】

【数 7 1】

- $p, q$ : prime numbers
  - $s \in \mathbf{Z} (gh^s \equiv 1 \pmod{n})$
- ... (数 7 1)

【 0 1 1 9 】

なる秘密情報  $(p, q, s)$  を作成し,

【 0 1 2 0 】

【数 7 2】

- $g, h, k \in \mathbf{Z} (0 < g, h < n)$
  - $n = pq$
- ... (数 7 2)

【 0 1 2 1 】

なる公開情報  $(n, g, h, k)$  (但し,  $k$  は  $p, q$  のビット長を表す。) を作成する。

【 0 1 2 2 】

受信者Bは、公開情報として  $n, g, h, k$  を通信回線300などを介して出力し、受信者側装置200へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関 (たとえば第3者側装置400) への登録など、周知の方法を用いることが可能である。その他の情報は、メモリ202に格納する。

【 0 1 2 3 】

## 2. 暗復号化处理

(1) 送信者側装置内の暗号化手段1004は、乱数生成手段1001を用いて整数  $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選ぶ。さらに、第3者あるいは、受信者側装置200から得られる上記公開情報2006と、べき乗算手段1002, 剰余演算手段1003とを用いて、送信データ  $m$  に対する暗号文  $C, D$  を

【 0 1 2 4 】

【数 7 3】

$$\begin{aligned} C &= mg^r \pmod{n}, \\ D &= h^r \pmod{n} \end{aligned}$$

... (数 7 3)

【0 1 2 5】

にて計算する。

【0 1 2 6】

さらに、暗号文 C, D を通信装置 103 を用いて通信回線 300 を介して受信者 B の受信者側装置 200 に送信する。

【0 1 2 7】

(2) 受信者側装置 200 において、復号化手段 2004 は、べき乗算手段 2002, 剰余演算手段 2003 と、保持されている上記秘密情報 2007 とを用いて、

【0 1 2 8】

【数 7 4】

$$m = CD^s \bmod n, \quad \dots (\text{数 } 74)$$

【0 1 2 9】

にて、暗号文 C, D から送信データ m を復号化する。

(実施例 5)

本実施例は、実施例 4 において、送信者の計算効率を高めるための鍵生成の方法について述べる。

【0 1 3 0】

受信者側装置 200 内の鍵生成手段 201 は、有限群  $G = \{x \in \mathbb{Z}/(n) \mid x \text{ は可逆元}\}$  の大きな位数  $L$  を持つ元  $\xi$  を選び (但し、 $\mathbb{Z}/(n)$  は  $n$  を法とする剰余環、 $L$  は  $\xi$  の位数の倍数でもよい)、整数  $\alpha, \beta$  に対して、

【0 1 3 1】

【数 7 5】

$$g = \xi^\alpha \bmod n, \quad h = \xi^\beta \bmod n \quad \dots (\text{数 } 75)$$

【0 1 3 2】

とする。さらに、

【 0 1 3 3 】

【数 7 6】

$$\alpha + s\beta \equiv 0 \pmod{L} \quad \dots (\text{数 } 7 \ 6)$$

【 0 1 3 4 】

となるように  $s$  を決める。

【 0 1 3 5 】

このとき、 $g$ 、 $h$ において、小さな整数  $k$  ( $k \geq 2$ ) に対して

【 0 1 3 6 】

【数 7 7】

$$h = g^k \bmod n \quad \dots (\text{数 } 7 \ 7)$$

【 0 1 3 7 】

とすると、送信者側の計算効率をさらに高めることができる。

【 0 1 3 8 】

また、公開鍵  $g, h$  が小さな値となるように  $p, q, \xi, \alpha, \beta$  を選ぶことにより、公開鍵のサイズを小さくすることが可能である。

【 0 1 3 9 】

より具体的には、 $\xi$  を大きな奇数（例えば素数） $L$  を位数とする小さな値を選び、 $\alpha = 1$ 、 $\beta = 2$  とする。このとき、

【 0 1 4 0 】

【数 7 8】

$$h = g^2 \bmod n \quad \dots (\text{数 } 7 \ 8)$$

【 0 1 4 1 】

となり、送信者側装置 100 内の暗号化手段 1004 は、べき乗算手段 1002、剰余演算手段 1003 を用いて、

【0 1 4 2】

【数 7 9】

$$W = g^r \bmod n$$

・・・(数 7 9)

【0 1 4 3】

を計算し、さらに、

【0 1 4 4】

【数 8 0】

$$C = mW \bmod n,$$

$$D = W^2 \bmod n$$

・・・(数 8 0)

【0 1 4 5】

により暗号文を計算することで、送信者側装置の計算負担を少なくすることが出来る。

【0 1 4 6】

(実施例 6)

本実施例は、実施例 4 において、受信者の計算効率を高めるための復号化方法について述べる。図 6 は本実施例の概要を示す。

【0 1 4 7】

受信者側装置 200 において、復号化手段 2004 は、べき乗算手段 2002、剰余演算手段 2003 と、保持されている上記秘密情報 2007 とを用いて、

【0 1 4 8】

【数 8 1】

$$m_1 = CD^s \bmod p,$$

$$m_2 = CD^s \bmod q$$

・・・(数 8 1)

【0 1 4 9】

を計算し、さらに

【 0 1 5 0 】

【数 8 2】

$$\begin{array}{lll} a \equiv 1 \pmod{p}, & a \equiv 0 \pmod{q}, & \dots (\text{数 } 8 \text{ 2}) \\ b \equiv 0 \pmod{p}, & b \equiv 1 \pmod{q} & \end{array}$$

【 0 1 5 1 】

なる整数  $a$ ,  $b$  に対して,

【 0 1 5 2 】

【数 8 3】

$$m = am_1 + bm_2 \pmod{n} \quad \dots (\text{数 } 8 \text{ 3})$$

【 0 1 5 3 】

にて, 暗号文  $C$ ,  $D$  から送信データ  $m$  を復号化する。

【 0 1 5 4 】

(実施例 7)

上記各実施例において,

【 0 1 5 5 】

【数 8 4】

$$g^r \pmod{n}, \quad h^r \pmod{n} \quad \dots (\text{数 } 8 \text{ 4})$$

【 0 1 5 6 】

の計算は暗号化対象である平文データ  $m$  に関係しないため, 前処理が可能である。すなわち, 送信者側装置 100 において, この計算を前処理として行い, その結果を上記メモリ 102 に保存しておき, 平文データ  $m$  を暗号化する時にその値を読み出して用いると, データ  $m$  を用いた処理のモジュラー積の個数は 1 個となるため, 暗号化時間を, さらに大幅に短縮する事が出来る。

【 0 1 5 7 】

(実施例 8)

本実施例は, 実施例 1 の変形例である。本実施例は, 実施例 3 と同様に, 送信者側の計算効率の向上を図るものである。

【0 1 5 8】

1. 鍵生成処理

予め、受信者側装置200内の鍵生成手段2001は、

【0 1 5 9】

【数 8 5】

- $p, q$ : prime numbers ... (数85)
- $s_0, s_1 \in \mathbb{Z}$

【0 1 6 0】

なる秘密情報  $(p, q, s_0, s_1)$  を作成し、

【0 1 6 1】

【数 8 6】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$  ... (数86)
- $n = p^d q (d \geq 1)$

【0 1 6 2】

なる公開情報  $(n, g, h, k)$

(但し、 $k$  は  $p, q$  のビット長を表す。また、 $s_i (i=1, 2)$  は、

【0 1 6 3】

【数 8 7】

$$s_i \alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1) \quad \dots \text{(数87)}$$

【0 1 6 4】

なる関係を満たす。) を作成する。

【0 1 6 5】

そして、上記公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ202に格納する。

【0 1 6 6】

## 2. 暗復号化处理

(1) 送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて、整数 $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選ぶ。さらに、送信データ $m$  ( $0 < m < 2^{k-1}$ ) について  $m = m_0 + m_1$  となるようにランダムに  $m_0, m_1$  を選ぶ。さらに、第3者側装置400あるいは受信者側装置200から得られる上記公開情報2006と、べき乗算手段1002、剰余演算手段1003を用いて、送信データ $m$ に対する暗号文 $C_0, C_1, D$ を

【0 1 6 7】

【数 8 8】

$$\begin{aligned} C_0 &= m_0 g^{\alpha_0 r} \bmod n, \\ C_1 &= m_1 g^{\alpha_1 r} \bmod n, \\ D &= g^{\beta r} \bmod n, \end{aligned} \quad \dots \text{(数 8 8)}$$

【0 1 6 8】

にて計算する。

【0 1 6 9】

さらに、暗号文 $C_0, C_1, D$ を通信装置103を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0 1 7 0】

(2) 受信者側装置200において、復号化手段2004は、保持している上記秘密情報2007と、べき乗算手段2002、剰余演算手段2003とを用いて、

【0 1 7 1】

【数 8 9】

$$m = C_0 D^{\beta_0} + C_1 D^{\beta_1} \bmod p \quad \dots \text{(数 8 9)}$$

【0 1 7 2】

にて、暗号文 $C_0, C_1, D$ から送信データ $m$ を復号化する。

【0 1 7 3】

また、送信者は暗号化处理の際、乱数 $r$ を導入しているため、本発明の方法は、確定的ではなく、確率的である。よって、新たに乱数情報を含ませることなく

，暗号文から平文の同一性を判断することは困難であり，文献 1 の方法などと比較して安全性を向上させている。

【0 1 7 4】

(実施例 9)

本実施例は，上記実施例で述べた方法に，一方向性関数を組み合わせるものである。これにより，送信者と受信者の間で鍵共有を行うこと(すなわち、共通鍵暗号方法に用いる鍵を配送すること)を可能にする。また、能動的な攻撃方法である選択暗号文攻撃を許さない環境を作り、能動的攻撃に対する安全性を確保する。

【0 1 7 5】

#### 1. 鍵生成処理

予め，受信者側装置200内の鍵生成手段2001は，

【0 1 7 6】

【数 9 0】

- $p, q$ : prime numbers ... (数 9 0)
- $s_0, s_1 \in \mathbb{Z}$

【0 1 7 7】

なる秘密情報  $(p, q, s_0, s_1)$  を作成し，

【0 1 7 8】

【数 9 1】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$  ... (数 9 1)
- $n = p^d q (d \geq 1)$
- $f$ : one-way function

【0 1 7 9】

なる公開情報  $(n, g, h, k, f)$

(但し， $k$  は  $p, q$  のビット長を表す。また， $s_i (i=1, 2)$  は，



【 0 1 8 0 】

【数 9 2】

$$s_i \alpha_i + \beta \equiv 0 \pmod{L} \quad (0 \leq i \leq 1) \quad \dots (\text{数 9 2})$$

【 0 1 8 1 】

なる関係を満たす。)を作成する。

【 0 1 8 2 】

そして、公開情報として $n, g, h, k, f$ を通信回線300などを介して出力し、受信者側装置200へ送付するか、または公開する。公開する方法として、たとえば公開情報管理機関（たとえば第3者側装置400）への登録など、周知の方法を用いることが可能である。その他の情報は、メモリ202に格納する。

【 0 1 8 3 】

## 2. 暗復号化处理

(1) 送信者側装置100内の暗号化手段1004は、乱数生成手段1001を用いて整数 $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選ぶ。さらに、送信データ $m$  ( $0 < m < 2^{k-1}$ ) について $m = m_0 + m_1$ となるようにランダムに $m_0, m_1$ を選ぶ。さらに、第3者側装置400あるいは受信者側装置200から得られる上記公開情報2006と、べき乗算手段1002、剰余演算手段1003を用いて、送信データ $m$ に対する暗号文 $C_0, C_1, D$ を

【 0 1 8 4 】

【数 9 3】

$$\begin{aligned} C_0 &= m_0 g^{\alpha_0 r} \bmod n, \\ C_1 &= m_1 g^{\alpha_1 r} \bmod n, \\ D &= g^{\beta r} \bmod n, \end{aligned} \quad \dots (\text{数 9 3})$$

【 0 1 8 5 】

にて計算する。

【 0 1 8 6 】

さらに、暗号文 $C_0, C_1, D$ を通信装置103を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

## 【0 1 8 7】

さらに、送信者側装置100内の一方向性関数手段2008は、公開情報である一方向性関数  $f$  から共通鍵  $K$  を  $K=f(m)$  により計算する。必要に応じて、アプリケーションAプログラム1005は、共通鍵  $K$  を用いて暗号化計算を行う。

## 【0 1 8 8】

(2) 受信者側装置200では、ICカード500内の復号化手段5004が、メモリ502に保持されている上記秘密情報2007と、べき乗算手段5002、剰余演算手段5003とを用いて、

## 【0 1 8 9】

## 【数9.4】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod p \quad \dots (数9.4)$$

## 【0 1 9 0】

にて、暗号文  $C_0, C_1, D$  から送信データ  $m$  を復号化する。

## 【0 1 9 1】

さらに、ICカード500内の一方向性関数手段5008は、公開情報である一方向性関数  $f$  から共通鍵  $K$  を  $K=f(m)$  により計算し、ICカード500から  $m$  を出力することなく、 $K$  を受信者側装置200に出力する。

## 【0 1 9 2】

受信者側装置200内のアプリケーションBプログラム2005は、この共通鍵  $K$  を用いて、同時に、あるいは、別途送付される、共通鍵  $K$  で暗号化されたデータを復号化する。

## 【0 1 9 3】

上述のように、本実施例は、実用的な一方向性関数を組み合わせて使用することにより、平文データ  $m$  ( $0 < m < 2^{k-1}$ ) を外部へ出力しない。

## 【0 1 9 4】

このように、ICカード(または、計算機カード)など個人が携帯する周辺機器内部で、暗号化、復号化処理を行うことで、選択暗号文攻撃を許さない、能動的攻撃に対しても安全な環境を作ることができる。

## 【0 1 9 5】

また、メッセージそのものを本発明による公開鍵暗号方法を用いて送信する構成においては、本実施例のアプリケーションBプログラム2005が、復号化したメッセージ（平文データ $m$ ）を所定の知識/ルールによって解釈して、意味のないメッセージが復号化されたと判断した場合、そのメッセージを秘密のうちに消去するなどして、他に知れないようにすることで、能動的攻撃を許さない環境を作ることが出来る。

## 【0 1 9 6】

上述のように、本実施例は、実用的な一方向性関数を組み合わせて使用することにより、さらに、能動的攻撃に対しても安全な環境を作るものである。

## 【0 1 9 7】

（実施例10）

本実施例は実施例 8 のさらなる変形例である。

実施例 8 に示した暗号化方法において、送信者側装置100の暗号化手段1004は、送信データ $m$  ( $0 < m < n$ ) に対して、暗号文( $C_0, C_1, D$ )を作成する。

## 【0 1 9 8】

受信者側装置200の復号化手段2004は、上記秘密情報2007と、べき乗算手段2002, 剰余演算手段2003とを用いて、

## 【0 1 9 9】

【数 9 5】

$$m = C_0 D^{s_0} + C_1 D^{s_1} \bmod n \quad \dots \text{(数 9 5)}$$

## 【0 2 0 0】

にて、暗号文( $C_0, C_1, D$ )から送信データ $m$ を復号化する。

## 【0 2 0 1】

本実施例では、送信データ $m$ の範囲を実施例 8 に比べて広く取れるため、実施例 8 に比べて長いメッセージを送ることが可能である。

## 【0 2 0 2】

（実施例 11）

実施例 8 および実施例 9 において、送信者側装置 100 の暗号化手段 1004 が、べき乗算手段 1002、剰余演算手段 1003 を用いて、

【0 2 0 3】

【数 9 6】

$$W = g^r \bmod n$$

・・・(数 9 6)

【0 2 0 4】

を計算し、さらに

【0 2 0 5】

【数 9 7】

$$g^{\alpha_i r} \bmod n = W^{\alpha_i} \bmod n \quad (0 \leq i \leq 1),$$

・・・(数 9 7)

$$g^{\beta r} \bmod n = W^{\beta} \bmod n$$

【0 2 0 6】

により、各々の値を計算することにより、効率的な暗号化処理が可能となる。

【0 2 0 7】

(実施例 12)

実施例 8 および実施例 10 において、

【0 2 0 8】

【数 9 8】

$$g^{\alpha_i r} \bmod n \quad (0 \leq i \leq 1), \quad g^{\beta r} \bmod n$$

・・・(数 9 8)

【0 2 0 9】

の計算は暗号化対象である平文データ  $m$  に関係しないため、前処理が可能である。すなわち、送信者側装置 100 において、この計算を前処理として行い、その結果を上記メモリ 102 に保存しておき、平文データ  $m$  を暗号化する時にその値を読み出して用いると、実施例 7 と同様に暗号化時間を、さらに大幅に短縮する事が出来る。

【0 2 1 0】

(実施例 13)

本実施例は、実施例 1 の変形例である。

【0 2 1 1】

まず、本実施例の概念は、送信者が、受信者の公開鍵を用いて送信データを暗号化し、受信者は前記公開鍵に対応する秘密鍵を用いて、暗号化された前記送信データを復号化する公開鍵暗号方法であって、

(1) 鍵情報生成のステップとして、

【0 2 1 2】

【数 9 9】

- $s \in \mathbb{Z}, gh^s = 1 (\in H)$  . . . (数 9 9)
- $H$ : subgroup of  $G$

【0 2 1 3】

なる前記秘密鍵  $(s, H)$  を作成し、さらに、

【0 2 1 4】

【数 1 0 0】

- $g, h \in G$  . . . (数 1 0 0)
- $G$ : finite group

【0 2 1 5】

なる前記公開鍵  $(g, h, G)$  を作成し、

(2) 前記送信者は、前記公開鍵  $(g, h, G)$  を用いて、乱数  $r$  を選び、前記送信データ  $m$  ( $m \in H$ ) について、暗号文  $C, D$  を

【0 2 1 6】

【数 1 0 1】

$$\begin{aligned} C &= m^t g^r (\in G), \\ D &= h^r (\in G) \end{aligned} \quad \dots (\text{数 } 101)$$

【0 2 1 7】

にて計算し、該暗号文  $C, D$  を前記受信者に送信し、

(3) 前記受信者は、前記秘密鍵  $(s, H)$  を用いて、

【0 2 1 8】

【数 1 0 2】

$$m^t = CD^s \ (\in H),$$

... (数102)

【0 2 1 9】

を計算し、これより前記送信データ $m$ を求めるものである。

【0 2 2 0】

以下、具体的な実施例について説明する。

【0 2 2 1】

#### 1. 鍵生成処理

受信者Bは、予め、受信者側装置200内の鍵生成手段2001を用いて、

【0 2 2 2】

【数 1 0 3】

- $p, q$ : prime numbers

... (数103)

- $s \in \mathbf{Z} \ (gh^s \equiv 1 \pmod{pq})$

【0 2 2 3】

なる秘密情報  $(p, q, s)$  を作成し、

【0 2 2 4】

【数 1 0 4】

- $g, h, k \in \mathbf{Z} \ (0 < g, h < n)$

... (数104)

- $n = p^d q \ (d \geq 1)$

【0 2 2 5】

なる公開情報  $(n, g, h, k)$  を作成し（但し、 $k$  は  $p, q$  のビット長を表す。）、公開情報を通信回線300などを介して出力し、送信者側装置100へ送付するか、または公開する。公開する方法として、例えば第3者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ202に格納する。

【 0 2 2 6 】

## 2. 暗復号化处理

(1) 送信者Aは、送信者側装置内の暗号化手段1004や乱数生成手段1001を用いて整数 $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選ぶ。さらに、第3者あるいは受信者Bから上記公開情報を得て、暗号化手段1004、べき乗算手段1002、剰余演算手段1003を用いて、送信データ $m$  ( $0 < m < 2^{k-1}$ ) から、暗号文 $C$ 、 $D$ を

【 0 2 2 7 】

【数 1 0 5】

$$\begin{aligned} C &= m^2 g^r \bmod n, \\ D &= h^r \bmod n \end{aligned} \quad \dots (\text{数} 1 0 5)$$

【 0 2 2 8 】

にて計算する。

【 0 2 2 9 】

さらに、暗号文 $C$ 、 $D$ を通信装置103を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 2 3 0 】

(2) 受信者Bは、保持している上記秘密情報と、受信者側装置200内の復号化手段2004、べき乗算手段2002、剰余演算手段2003を用いて、

【 0 2 3 1 】

【数 1 0 6】

$$m^2 = CD^s \bmod pq, \quad \dots (\text{数} 1 0 6)$$

【 0 2 3 2 】

を計算し、これより送信データ $m$ を復号化する。ここで、 $m$ を計算する手段としては、文献3や文献「Berlekamp, E.R.: Factoring Polynomials over Finite Field, Bell. Sys. Tech. J. 46, pp.1853-1859 (1967)」による方法の他、 $n$ がBlum数の場合における簡単な計算方法、などが知られている。また、これらの方法により得られた複数解を一意的に選択する方法も幾つか知られている（文献「岡本，山本：現代暗号，産業図書」）。

## 【0 2 3 3】

上記方法を用いれば、文献 3 にて開示されているものと同様の考察により、ある前提の下で、受動的攻撃に対して暗号文から平文を求めること（完全解読）は、 $n$  を素因数分解することよりも困難であることを証明することができる。

## 【0 2 3 4】

証明のアウトラインについて以下に述べる。

## 【0 2 3 5】

本実施例による方式が完全解読できたとすると、 $n$  の素因数分解ができることを示す。本実施例で述べた方法が破るアルゴリズム I が存在したと仮定する。このとき、このアルゴリズム I を利用して  $n$  の素因数分解を行うアルゴリズムを次のように構成できる。 $c$  なる  $m'$  を選び、ランダムな整数  $r'$  に対し、暗号文  $(C', D')$  を、

## 【0 2 3 6】

## 【数 1 0 7】

$$\begin{aligned} C' &= m'^2 g^{r'} \bmod n, \\ D' &= h^{r'} \bmod n \end{aligned} \quad \dots (\text{数 } 107)$$

## 【0 2 3 7】

にて作成する。このとき、暗号文  $(C', D')$  をアルゴリズム I に入力して、平文  $m$  を計算する。このとき、無視できない確率で  $m$ （または、 $m'$ ）の範囲に複数の解が存在するとき、 $m - m' (\neq 0)$  と  $n$  の公約数を調べることにより、 $n$  の素因数分解を行うことが出来る。素因数分解問題は NP 問題であり、効率よく解くアルゴリズムは存在しないことが十分に議論された上で予想されているため、上記方法による暗号通信の安全性が保証することができる。

## 【0 2 3 8】

また、上記方法を用いれば、semantic security が Diffie-Hellman 決定問題の困難性のもとで実施例 1 の場合と同様にして示すことができる。

## 【0 2 3 9】

以上述べたように、本発明の方法は受動的攻撃に対する安全性を保証することができる。



## 【 0 2 4 0 】

また、送信者は暗号化処理の際、乱数 $r$ を導入しているため、本発明の方法は、確定的ではなく、確率的である。よって、新たに乱数情報を含ませることなく、暗号文から平文の同一性を判断することは困難であり、文献 1 の方法などと比較して安全性を向上させている。

## 【 0 2 4 1 】

## (実施例 14)

本実施例は、上記実施例 1 3 で述べた概念とその具体的な方法に対して、実施例 2 などと同様な一方向性関数を組み合わせるものである。これにより、送信者と受信者の間で鍵共有を行うこと（例えば、共通鍵暗号方法に用いる鍵の配送）を可能にする。また、能動的攻撃方法である選択暗号文攻撃を許さない環境を作り、能動的攻撃に対する安全性を確保する。

## 【 0 2 4 2 】

## 1. 鍵生成処理

受信者 B は、予め、受信者側装置 200 内の鍵生成手段 2001 を用いて、

## 【 0 2 4 3 】

## 【数 1 0 8】

- $p, q$ : prime numbers ... (数 1 0 8)
- $s \in \mathbb{Z} (gh^s \equiv 1 \pmod{pq})$

## 【 0 2 4 4 】

なる秘密情報  $(p, q, s)$  を作成し、

## 【 0 2 4 5 】

## 【数 1 0 9】

- $g, h, k \in \mathbb{Z} (0 < g, h < n)$
- $n = p^d q (d \geq 1)$  ... (数 1 0 9)
- $f$ : one-way function

## 【 0 2 4 6 】

なる公開情報  $(n, g, h, k)$  を作成し（但し、 $k$  は  $p, q$  のビット長を表す。）、公開情報を通信回線 300 などを通して出力し、送信者側装置 100 へ送付するか、ま

たは公開する。公開する方法として、例えば第3者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ202に格納する。

## 2. 暗復号化处理

(1) 送信者側装置100内の乱数生成手段1001を用いて整数 $r$  ( $0 < r < 2^{k-1}$ ) をランダムに選ぶ。さらに、第3者あるいは受信者Bから上記公開情報を得て、暗号化手段1004、べき乗算手段1002、剰余演算手段1003を用いて、送信データ $m$  ( $0 < m < 2^{k-1}$ ) から、暗号文 $C$ ,  $D$ を

【0 2 4 7】

【数 1 1 0】

$$C = m^2 g^r \bmod n,$$

$$D = h^r \bmod n$$

・・・(数110)

【0 2 4 8】

にて計算する。

【0 2 4 9】

さらに、暗号文 $C$ ,  $D$ を通信装置103を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0 2 5 0】

送信者Aは、送信者側装置100内の一方向性関数手段2008は、公開情報である一方向性関数 $f$ から共通鍵 $K$ を $K=f(m)$ により計算する。

【0 2 5 1】

(2) 受信者Bは、ICカード500内にて保持している上記秘密情報2007と、ICカード500内の復号化手段5004、べき乗算手段5002、剰余演算手段5004を用いて、

【0 2 5 2】

【数 1 1 1】

$$m^2 = CD^s \bmod pq,$$

・・・(数111)

【0 2 5 3】

を計算し、これより送信データ $m$ を復号化する。さらに、受信者BはICカード50

0内の一方向性関数手段5008を用いて、公開情報である一方向性関数  $f$  から共通鍵  $K$  を  $K=f(m)$  により計算し、共通鍵  $K$  を受信者側装置に出力する。

上述の様に、本実施例では、一方向性関数を組み合わせて、使用することにより、送信データ  $m$  自身は外部へ出力しない。このように、ICカード（または、計算カード）など個人が携帯する周辺機器内部で、暗号化および復号化を行うことで、選択暗号文攻撃を許さない、すなわち、能動的攻撃に対しても安全な環境を作ることができる。

#### 【0 2 5 4】

また、メッセージそのものを本発明による公開鍵暗号方法を用いて送信する構成においては、本実施例のアプリケーションBプログラム2005が復号化したメッセージを所定のルールによって解釈し、意味のないメッセージが復号されたと判断した場合、そのメッセージを外部機器に出力することなく消去するなどして、能動的攻撃を許さない環境を作ることができる。

#### 【0 2 5 5】

上述のように、本実施例は一方向性関数を組み合わせて使用することにより、さらに、能動的攻撃に対しても安全な環境を作るものである。

#### 【0 2 5 6】

(実施例15)

本実施例は実施例 1 3 の基本形である。

#### 【0 2 5 7】

実施例 1 3 において、 $d=1$  とし、送信者は、送信データ  $m$  ( $0 < m < n$ ) に対して、前記暗号化方法にて暗号文  $C, D$  を作成し、暗号文  $C, D$  を受信者に送信する。

#### 【0 2 5 8】

受信者は、保持している上記秘密情報2007と、受信者側装置200内の復号化手段2004、べき乗算手段2002、剰余演算手段2003を用いて、

#### 【0 2 5 9】

【数 1 1 2】

$$m^2 = CD^s \bmod n, \quad \dots (\text{数} 1 1 2)$$

## 【0260】

にて、暗号文C、Dから送信データmを復号化する。

## 【0261】

本実施例による方法では、前提を置くことなく、完全解読の困難性と素因数分解問題の困難性の等価性、および、部分解読の困難性とDiffie-Hellman決定問題の困難性の等価性を示すことができる。

## 【0262】

また、本実施例では、送信データmの範囲を実施例13に比べて広く取れるため、実施例13に比べて長いメッセージを送ることが可能である。

## 【0263】

(実施例16)

実施例7と同様に、実施例13から実施例15においても、

## 【0264】

【数113】

$$g^r \bmod n, \quad h^r \bmod n \quad \dots \text{(数113)}$$

## 【0265】

の計算は、送信データmに関係しないため、前処理が可能である。これにより、暗号化時間を大幅に短縮することが可能となる。

## 【0266】

なお、すでに述べたように、上記各実施例において、 $d$  ( $d \geq 1$ ) の値を  $n$  の素因数分解が困難である範囲において、大きく選ぶことで、 $n$  のビット数が一定の場合、 $p$  のビット数が小さくなるため、復号化処理を高速に行うことが出来る。この  $d$  の値を、第3者側装置あるいは、受信者側装置にて管理すれば、計算機能力の発展、素因数分解に必要とされる計算時間と安全性との関係などによって、変えることが可能である。

## 【0267】

また、上記各実施例における送信データmには、通常の秘密に送信したいメッセージのほか、共通鍵暗号方法に用いる共通鍵、メッセージ認証に用いるメッセ

ージとメッセージ認証子を合わせたものが当てはまる。

【 0 2 6 8 】

また、本実施例では、送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが、具体的には様々なシステムに適用される。

【 0 2 6 9 】

例えば、電子ショッピングシステムでは、送信者はユーザであり、送信者側装置はパソコンなどの計算機であり、受信者は小売店、受信者側装置はパソコンなどの計算機となる。このとき、ユーザの商品等の注文書は共通鍵暗号方法で暗号化されることが多く、その際は、暗号化鍵を本発明による鍵共有（鍵配送）方法により暗号化して小売店側装置に送信される。

【 0 2 7 0 】

また、電子メールシステムでは、各々の装置はパソコンなどの計算機であり、送信者のメッセージは共通鍵暗号方法で暗号化されることが多い。その際も、暗号化鍵は、本発明による鍵共有（鍵配送）方法を用いて暗号化して受信者の計算機に送信される。

【 0 2 7 1 】

その他にも、従来の公開鍵暗号が使われている様々なシステムに適用することが可能である。

【 0 2 7 2 】

なお、本実施例における各計算は、CPUがメモリ内の各プログラムを実行することにより行われるものとして説明したが、プログラムではなく、いずれかがハードウェア化された演算装置であって、他の演算装置やCPUと、データのやりとりを行うものであってもよい。

【 0 2 7 3 】

【発明の効果】

本発明によれば、安全で、高速処理が可能な、公開鍵暗号方法と、その応用装置、システムを実現することができる。

【図面の簡単な説明】

【図 1】

本発明の各実施例のシステム構成を示す図である。

【図 2】

本発明の実施例における IC カードの内部構成を示す図である。

【図 3】

本発明の実施例 1 の概要を示す図である。

【図 4】

本発明の実施例 3 の概要を示す図である。

【図 5】

本発明の実施例による方式と代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）の比較を表す図である。

【図 6】

本発明の実施例 6 の概要を示す図である。

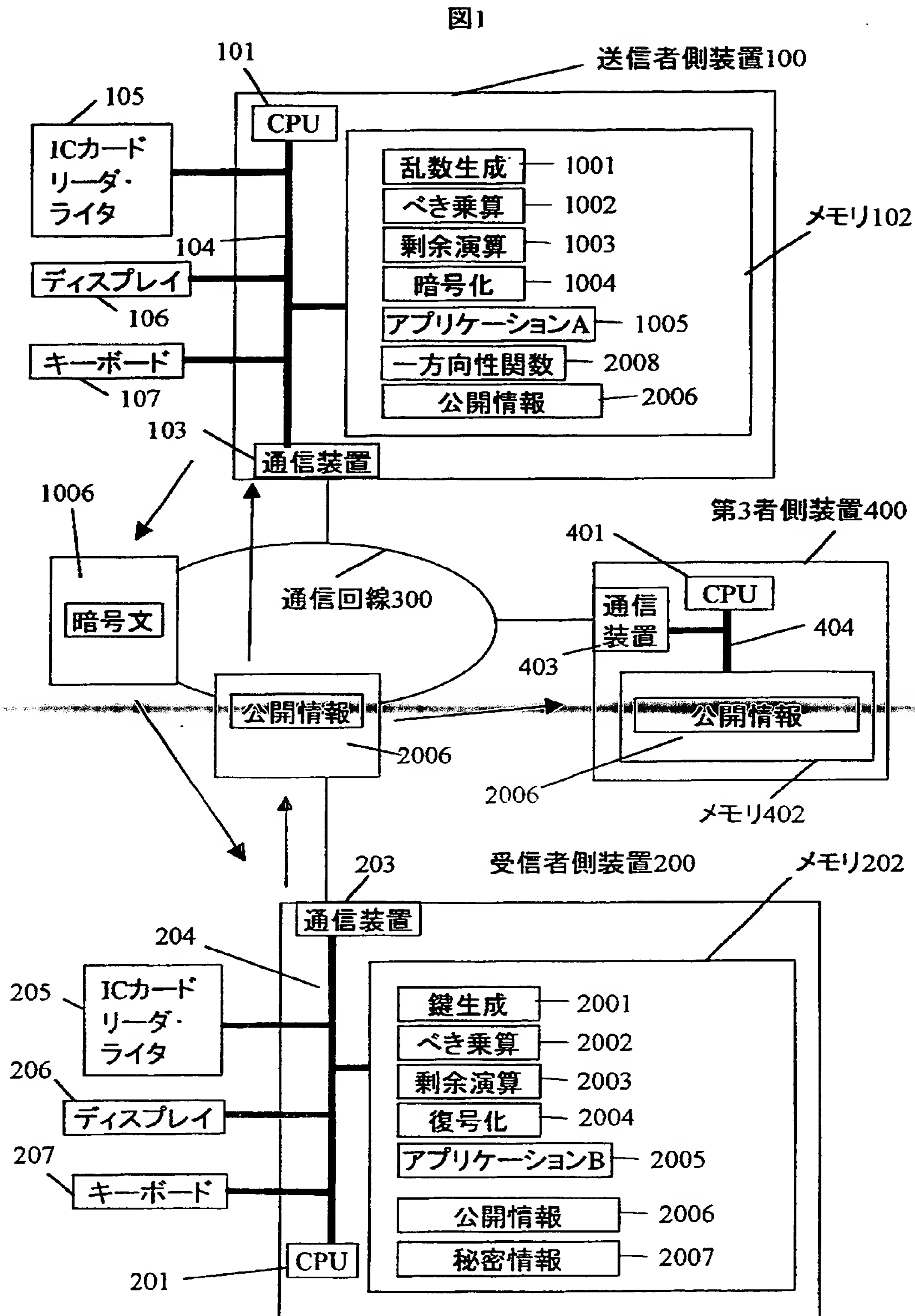
【符号の説明】

1 0 0 …送信者側装置, 1 0 1 …送信者側装置 1 0 0 内の CPU, 1 0 2 …送信者側装置 1 0 0 内のメモリ, 1 0 3 …送信者側装置 1 0 0 内の通信装置, 1 0 0 1 …送信者側装置 1 0 0 内の乱数生成手段, 1 0 0 2 …送信者側装置 1 0 0 内のべき乗算手段, 1 0 0 3 …送信者側装置 1 0 0 内の剰余演算手段, 1 0 0 4 …送信者側装置 1 0 0 内の暗号化手段, 2 0 0 …受信者側装置, 2 0 1 …受信者側装置 1 0 0 内の CPU, 2 0 2 …受信者側装置 2 0 0 内のメモリ, 2 0 3 …受信者側装置 2 0 0 内の通信装置, 2 0 4 …受信者側装置 2 0 0 内の IC カードリーダー/ライター, 2 0 0 1 …受信者側装置 2 0 0 内の鍵生成手段, 2 0 0 2 …受信者側装置 2 0 0 内のべき乗算手段, 2 0 0 3 …受信者側装置 2 0 0 内の剰余演算手段, 2 0 0 4 …受信者側装置 2 0 0 内の復号化手段, 2 0 0 6 …公開情報, 2 0 0 7 …秘密情報, 5 0 0 …受信者の IC カード, 5 0 1 …IC カード 5 0 0 内の CPU, 5 0 2 …IC カード 5 0 0 内のメモリ, 5 0 3 …IC カード 5 0 0 内の I/O, 5 0 0 1 …IC カード 5 0 0 内の鍵生成手段, 5 0 0 2 …IC カード 5 0 0 内のべき乗算手段, 5 0 0 3 …IC カード 5 0 0 内の剰余演算手段, 5 0 0 4

… I C カード 5 0 0 内の復号化手段, 5 0 0 8 … I C カード 5 0 0 内の一方向性関数手段。

【書類名】 図面

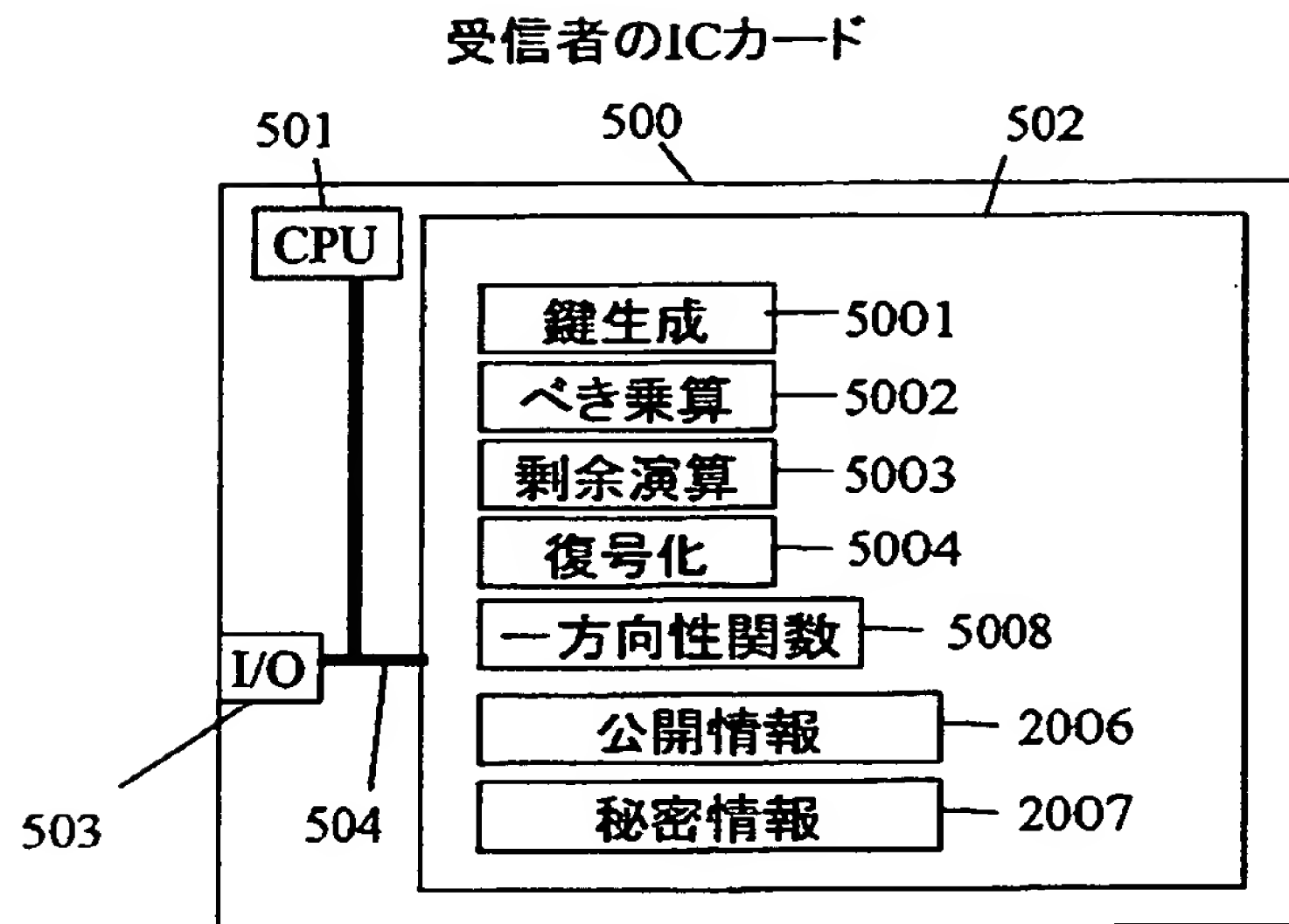
【図 1】





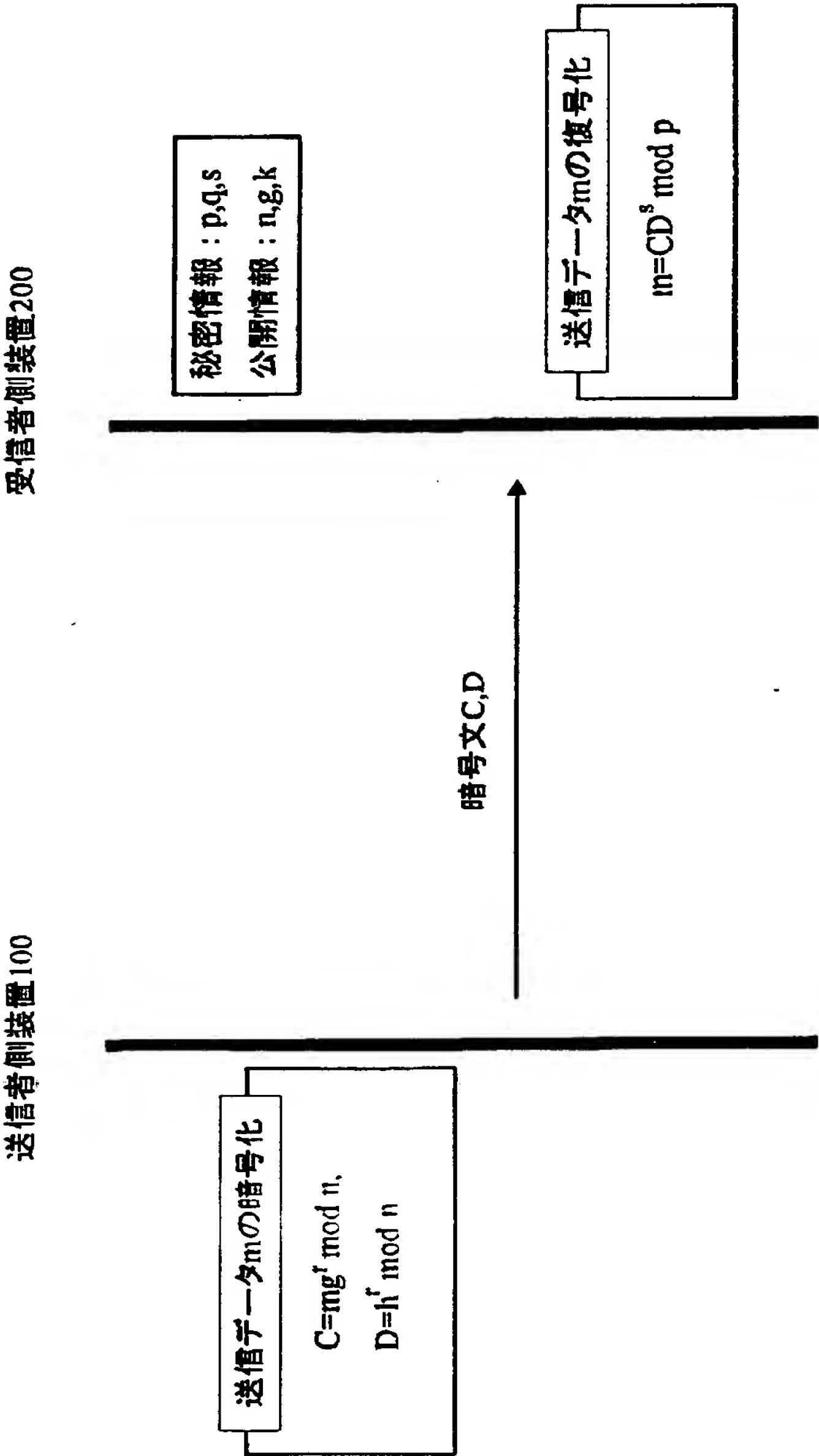
【図 2】

図2



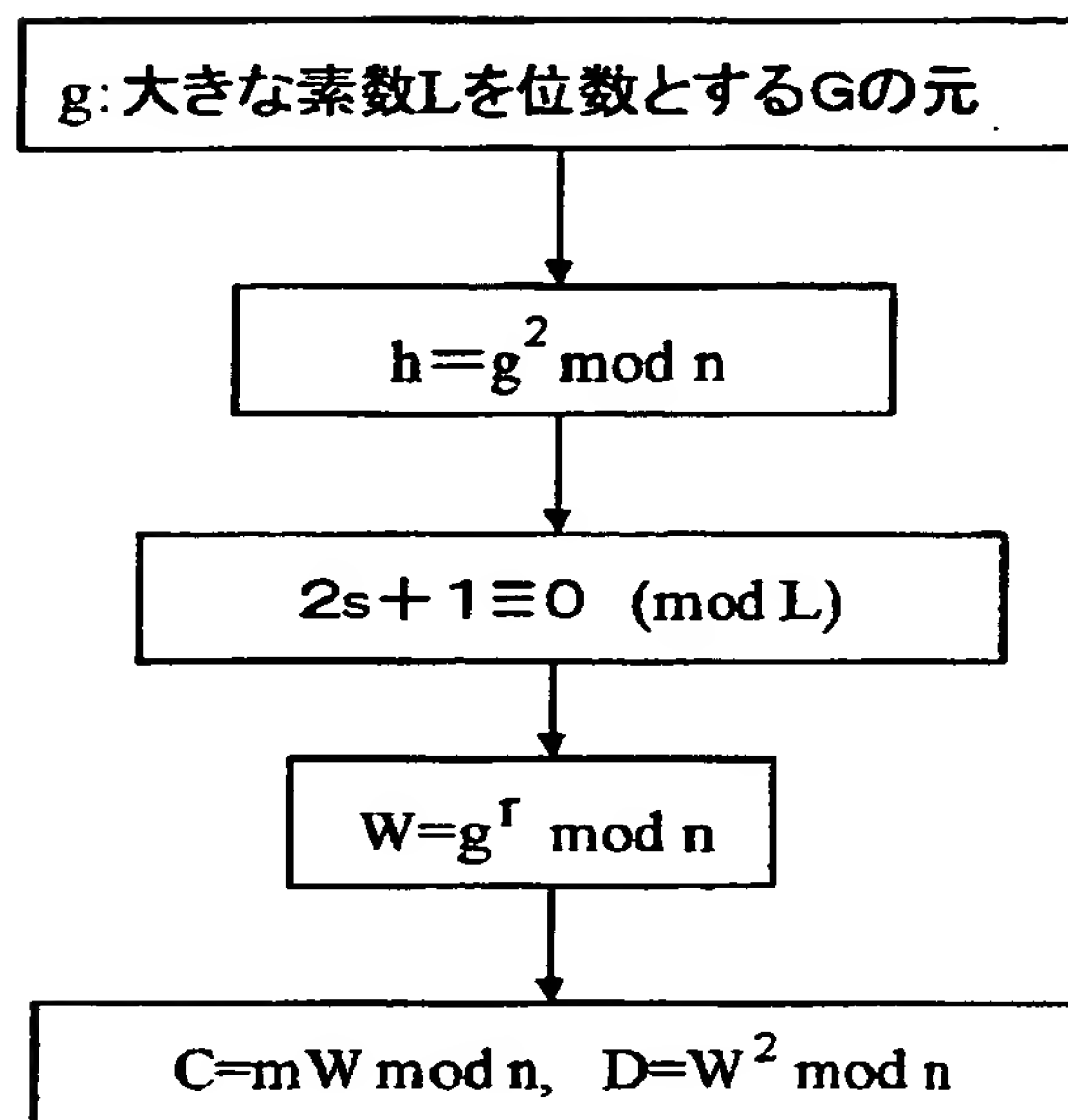
【図 3】

図3



【図 4】

図 4



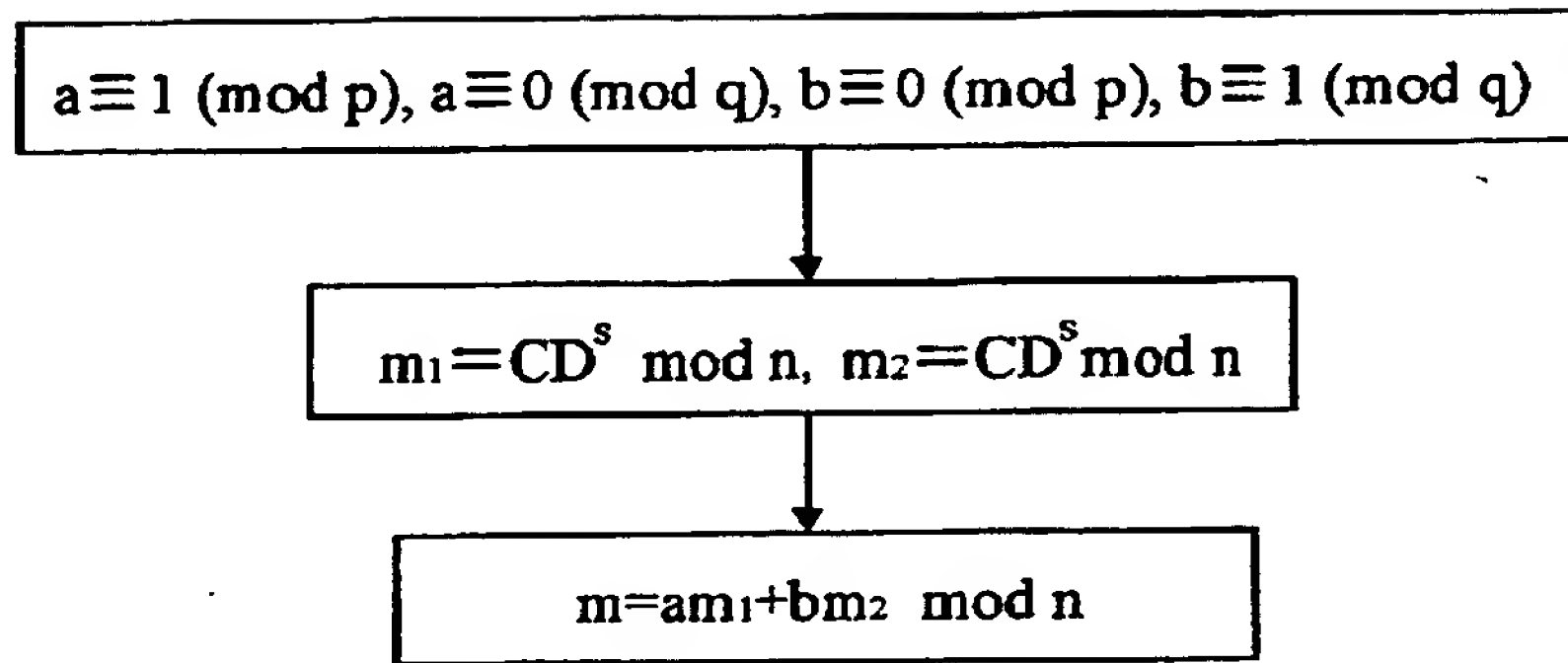
【図 5】

図 5

	暗号化	復号化
RSA	約 2~1500	約 400
ElGamal暗号	約 3000	約 1500
EPE	約 13	約 400
EPOC	約 230	約 230
本発明の方式	約 200	約 60

【図 6】

図6



【書類名】 要約書

【要約】

【課題】

受信者の公開鍵を用いて、送信データを暗号化する公開鍵暗号による暗号通信方法であって、安全性の証明が可能であり、かつ、効率性の高い処理ができる公開鍵暗号方法および装置を提供する。

【解決手段】

受信者は、受信者側装置200を用いて、秘密鍵として $(p, q, s)$ を作成し、公開鍵として $(n, g, k)$ を作成する（但し、 $k$ は $p, q$ のビット長）。

送信者は、送信者側装置100を用いて、乱数 $r$  ( $0 < r < 2^{k-1}$ ) を選び、送信データ $m$  ( $0 < m < 2^{k-1}$ ) について、 $C = mg^r \bmod n$ ,  $D = g^{2r} \bmod n$ を計算して、暗号化する。

受信者は、受信者側装置200を用いて、暗号文 $C$ 、 $D$ について $m = CD^s \bmod p$ により、送信データ $m$ に復号化する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地

氏 名 株式会社日立製作所

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

This Page Blank (uspto)